ABSTRACT

A network architecture for console-based gaming systems enables secure communication among multiple game consoles over a local area network. The system architecture supports a three-phase secure communication protocol. The first phase involves generating shared keys that are unique to an authentic game console running an authentic game title. In the second phase, a "client" console attempts to discover existing game sessions being hosted by a "host" game console by broadcasting a request over the local area network. The broadcast request is protected using the shared keys. If the host console agrees to let the client console play, the host console generates session keys that are returned to the client console. The third phase involves a key exchange in which the client and host consoles exchange data used to derive one or more secrets for securing future communications. The key exchange is protected using the session keys.